International Journal of Computer Applications Technology and Research
Volume 13–Issue 11, 30 – 34, 2024, ISSN:-2319–8656
DOI:10.7753/IJCATR1311.1005

IoT Based Surveillance Model for Monitoring School Children

Irvin Kiplagat Kilot
Student
Kabarak University
Nakuru, Kenya

Dr. Nelson Masese
Lecturer
Kabarak University
Nakuru, Kenya

Prof. Simon Maina Karume
Lecturer
Kabarak University
Nakuru, Kenya

Abstract: Due to their inherent vulnerability, reliance on caregivers, and limited understanding of potential hazards and self-defense, children are naturally prone to accidents, exploitation, and various forms of abuse. Recent media coverage has shown an alarming increase in crimes targeting children, including abductions and murders, intensifying concerns about child safety. Because children spend a majority of their time in school, it is the joint duty of both the school and parents to ensure the continuous monitoring and care of children. The popular method of accounting for children in Kenyan schools is by performing a physical head count and checking of class lists. This process can be long, tiresome and hard to maintain for the those concerned. Furthermore, the process is not efficient enough for the school to know whether students are absent from classes during the course of the day. To improve the situation, surveillance of children has to be done properly and efficiently. In order to address the challenges related to monitoring and ensuring the attendance and safety of learners, it becomes imperative to embrace current technology. Technologies such as Global Positioning System, Radio-Frequency Identification, Ultra Wide Band, Bluetooth Low Energy, Infrared, Wi-Fi and Zigbee and have been employed in object tracking scenarios. The general term given to these devices is Internet of Things(IoT). The utilization of IoT offers numerous possibilities for enhancing student, including the ability to track students' movements within the school premises. Consequently, this research will concentrate on the development of an IoT-based surveillance system for monitoring school children. weaknesses of IoT based surveillance models for monitoring children.
Keywords Child safety, School children, Surveillance, Internet of Things (IoT), Real-time tracking.

1.0 INTRODUCTION

The Constitution of Kenya [1] guarantees children the right to free and compulsory basic education while protecting them from abuse, neglect, violence, exploitative labor, and harmful cultural practices. As part of this mandate, parents, teachers, and school management are tasked with ensuring the safety of children in learning environments. Teachers, in particular, are responsible for monitoring students' whereabouts to prevent unauthorized exits or concealment on school premises, behaviors that may compromise children's safety and create anxiety for both staff and parents [2].

Given the growing safety concerns in schools, there is a pressing need for more effective monitoring solutions to protect children within and beyond school premises. One promising solution is the use of Internet of Things (IoT) technologies, which can offer enhanced visibility into student activities and attendance. A study conducted in Iraqi primary schools demonstrated that IoT-based systems could help address challenges in monitoring students' attendance and safety [3]. IoT technologies—such as GPS, RFID, and Wi-Fi—enable the interconnection of physical objects with the internet, facilitating access to real-time data from sensors and other devices [4].

The integration of IoT technologies into child monitoring systems offers significant benefits. For instance, real-time location tracking using GPS and RFID can provide instant alerts when children exit designated areas, allowing caregivers to take timely action [5]. Wearable devices and smart tags further enhance child safety by offering immediate feedback on children's movements and activities, ensuring that interventions can occur swiftly when needed [6], [7]. For children with special needs, IoT systems enable personalized monitoring and adaptive learning experiences, promoting better developmental outcomes through tailored support [8].

Beyond location tracking, IoT technologies can also support children's health by monitoring vital signs and environmental conditions, enabling the early detection of abnormalities [9]. These features not only ensure safety but also promote well-being by integrating health monitoring into daily activities. However, despite its numerous advantages, the implementation of IoT-based child monitoring systems presents several challenges.

One of the foremost concerns is data security. Systems that handle sensitive information, such as children's location or health data, are vulnerable to privacy breaches and cyberattacks [10]. Ensuring that such personal data remains protected is critical in both school and home environments, where IoT systems operate continuously [11]. Scalability is another challenge, as IoT devices generate vast amounts of real-time data, creating complexities in data management, storage, and processing [12].

Moreover, there are concerns about the potential over-reliance on technology, which may reduce meaningful human interaction and impede the social development of young children. While IoT systems are valuable tools, they must complement—not replace—human supervision, ensuring that children's emotional and developmental needs are met [8].

In conclusion, while IoT offers promising solutions for improving child monitoring through features such as real-time tracking, personalized support, and health monitoring, these benefits must be carefully balanced with the associated risks. Addressing challenges related to security, scalability, and the need for human oversight is essential to ensure that IoT technologies are integrated safely and effectively. As these technologies continue to evolve, ongoing research is crucial to better understand their long-term effects on child development and to ensure that IoT solutions support—not hinder—the well-being of children [5].

1.1 Current Child Monitoring Methods In Kenya

In Kenya, concerns about child safety have risen sharply due to the increasing rates of kidnappings and crimes targeting children. Many parents have taken legal action against schools when children have gone missing, emphasizing the urgent need for effective monitoring systems. Day scholar students often either arrive at school and then sneak out or fail to reach the school premises altogether. Schools, being responsible for the safety of their students, must have a reliable way to verify each child's presence and promptly notify parents when a child is absent at the start of the school day. However, the systems currently in place, primarily relying on RFID tags, lack the efficiency needed to track student movements accurately.

Traditional attendance methods like physical headcounts and roll calls are still common but are time-consuming, cumbersome, and difficult to manage, leading to gaps in monitoring students' presence. Consequently, schools often remain unaware when students are absent from class. To address these issues, a solution is needed that not only tracks children within school premises but also detects attempts to leave unauthorized areas.

This study proposed a more advanced child monitoring model using IoT technology to enhance safety through real-time location tracking and alert systems. By automatically monitoring a child's movements within school boundaries and sending alerts when a child exits during school hours, the IoT-based surveillance model aims to deter crimes, prevent unauthorized activities, and alleviate parents' concerns about their children's safety. The objective of this paper is to analyze the weaknesses of existing IoT based surveillance models for monitoring children

2.0 LITERATURE REVIEW

2.1 Internet of Things

Technological advancements have introduced new concepts, including the Internet of Things (IoT). Coined by Kevin Ashton in 1999, IoT refers to a global network infrastructure that connects physical devices to the internet, enabling seamless information exchange and smart recognition [13]. IoT facilitates interconnection between physical objects and virtual systems, allowing data to flow continuously, regardless of time or location.

IoT plays a crucial role across technological, social, and economic domains, revolutionizing how we interact with everyday objects. Connected devices are now integrated into consumer products, vehicles, and industrial equipment, transforming industries with data-driven capabilities [14]. Examples include smart homes, which enhance energy efficiency and security, and healthcare solutions such as wearable health monitors, improving personal and medical outcomes [14].

A core element of the IoT ecosystem is the IoT platform, which ensures the smooth interaction of devices. These platforms, often called middleware, bridge the gap between hardware and applications, handling data collection, device management, and remote configuration. They also provide essential features such as over-the-air firmware updates, cloud connectivity, and security to support the rapid development of IoT applications [15].

The essence of IoT lies in its ability to turn everyday objects into intelligent tools capable of collecting, transmitting, and acting on data without human intervention. By equipping devices with sensors and internet connectivity, IoT fosters autonomous decision-making, driving innovations in smart cities, transportation, healthcare, and more [15]. As IoT evolves, it will create a more interconnected world, reshaping various aspects of daily life and delivering personalized experiences [15].

Sensors are the backbone of IoT, gathering data for processing and control. In surveillance, GPS, RFID, and GSM technologies ensure reliable, real-time tracking for child safety and other monitoring applications, enhancing accuracy and system performance [14].

2.2 Existing IoT Child Monitoring Systems

The IoT-based school attendance system using RFID technology automates attendance management in three phases: detection using UHF RFID readers, real-time notification via SMS/email, and dissemination of missed lessons for absent students. This model eliminates teacher intervention in attendance recording, improving efficiency and transparency between schools and parents. The system's ability to email missed lessons fosters continuity in education, and its success prompted the suggestion to expand IoT usage to high school guidance systems [13].

Ahmed et al. proposed a school bus tracking system with dual authentication using fingerprint and RFID for enhanced student security. Real-time location tracking, accessible through an Android app, informs parents of their child's whereabouts, mitigating anxiety. The model also prevents students from disembarking at unauthorized locations by repeating authentication during drop-offs. This system highlights the importance of security and real-time updates for parents, particularly in urban settings like Dhaka [16].

A touch-free attendance system was proposed, integrating RFID, infrared thermometers, and ultrasonic sensors for a contactless experience [17]. Particularly relevant during the COVID-19 pandemic, this system checks both student presence and body temperature, automating alerts for fever detection. The use of cloud storage for attendance and health data enables remote monitoring and reporting, making it a flexible and scalable solution for schools [17].

An IoT-based school bus monitoring system that integrates real-time tracking, RFID-based learner detection, and multiple safety sensors for speed, intoxication, and smoke detection was developed [18]. The system mitigates risks by alerting parents and school authorities to unsafe conditions. Continuous data collection ensures proactive decision-making regarding bus safety, offering a comprehensive safety solution for student transport [18].

The student monitoring system by Maturkar et al. ensures safety during school bus transit using RFID and GSM technology for real-time updates to parents about their child's location. The system also incorporates safety features like speed control, temperature sensors, and alcohol detection for the driver, ensuring a safe transit environment. The SMS-based communication makes this a cost-effective solution for parents to monitor their child's safety [19].

Tesfaye proposed a real-time child monitoring system using a GPS-enabled smart tag that continuously updates parents about their child's location and activities, categorized into statuses like "Studying" or "Dangerous" [20]. The system alerts parents if their child strays from the school compound or follows an unexpected route. This affordable solution emphasizes child

safety through continuous GPS tracking and real-time alerts [20].

Senthamilarasi et al. developed a comprehensive IoT-based child safety system that integrates GPS, geofencing, temperature, and pulse sensors to monitor child movement and health. The system's real-time tracking and sensor-based health monitoring provide instant alerts to parents, and live video streaming enhances monitoring by offering visual confirmation of the child's safety [9]. This model represents a significant advancement in ensuring child safety [21].

2.3 Challenges in Implementing Child Monitoring Systems

Implementing IoT in child monitoring systems presents several challenges. One challenge is the data resolution of wearable sensors. These compact sensors, designed for children's comfort, often have lower resolution, which can compromise tracking accuracy [22]. Power consumption is another issue; as wearable devices need to operate for long periods without frequent battery changes. Energy-efficient designs like solar power are helpful but limited by indoor and nighttime conditions [23].

The wearability of IoT devices is also critical; they must be lightweight yet functional, balancing comfort with computational capabilities [24]. Safety concerns arise due to radiofrequency radiation from wireless technologies, especially near sensitive areas [22]. Security is a major concern, as low-power IoT devices often lack robust security features, making them vulnerable to hacking [25]. Regulatory gaps further complicate implementation, with a lack of standardized rules hindering deployment across different regions [22]. Finally, privacy risks exist due to constant data exchange, necessitating stronger privacy protocols to protect sensitive information [25]. Addressing these challenges is crucial for effective and secure IoT-based child monitoring systems.

3.0 RESEARCH METHODOLOGY

To achieve the objective of the research systematic literature review was employed as a research methodology to analyze the effectiveness of existing models. This involved a systematic investigation relying on existing data throughout the research process. This approach entailed organizing, collating, and analyzing available data sources to draw valid research conclusions. Often referred to as secondary research or desk research, this methodology involved synthesizing data from various sources such as the internet, peer-reviewed journals, textbooks, government archives, and libraries.

By conducting a systematic literature review, it was possible to critically evaluate the strengths and weaknesses of existing IoT-based surveillance models for monitoring children. This methodology allowed for a comprehensive examination of the literature, which was helpful in designing a conceptual model for the research. It served as an initial step to identify areas that required further investigation and informed the subsequent research stages.

4.0 RESULTS

4.1 Weaknesses of the Existing Models

To understand the value of a technology product, there must be a clear purpose for its existence. Thus, to justify the creation of a new IoT Surveillance model, the current real-world alternatives must demonstrate inefficiencies in their applications. The criteria set for evaluating these existing models encompass: the accuracy and reliability of detection, system scalability, flexibility in integration, data security, cost-effectiveness in both initial setup and ongoing operations, ease of use and maintenance, adaptability to different environments, and customizability. Additionally, the system's functionality, including its feature set and overall performance, must be thoroughly evaluated. The table below shows a generalized analysis of the weaknesses of models according to assessment criterion.

Table 1. Generalized Weaknesses of Models According to Assessment Criteria

Assessment Criterion	Generalized Weaknesses
Accuracy and Reliability	Models often rely on RFID tags or biometric sensors, which can fail due to environmental interference, damaged hardware, or improper calibration. This results in missed detections or false readings.
System Scalability	Many systems struggle to scale effectively, especially when integrating multiple devices and handling increased data. Larger deployments introduce complexity in infrastructure and risk performance degradation.
Flexibility in Integration	Integration challenges arise from the use of proprietary or specific technologies (e.g., RFID, GSM). These technologies often limit interoperability with existing school management systems or future upgrades.
Data Security	Weak encryption, lack of robust authentication protocols, and reliance on SMS for data transmission expose sensitive information to risks such as interception, unauthorized access, and data breaches.
Cost-Effectiveness	Initial setup and maintenance costs are high due to hardware requirements (e.g., RFID readers, sensors, microcontrollers). These costs can limit adoption in budget-constrained environments.
Ease of Use and Maintenance	Systems with multiple components require ongoing maintenance, calibration, and technical expertise, which can burden users, especially in schools with limited staff training and resources.
System Functionality and Performance	Functionality depends on the seamless operation of various components. Issues such as poor network connectivity, incompatible modules, or device malfunctions negatively impact performance.

Below are design recommendations derived from the generalized weaknesses of models according to the assessment criteria:

Table 2. Design recommendations derived from the generalized weaknesses

Assessment Criterion	Design Recommendations

Accuracy and Reliability	Implement redundancy by combining multiple detection technologies (e.g., RFID with GPS) to minimize false readings. Introduce periodic calibration routines and self-diagnostic tools to identify faulty hardware promptly. Enhance algorithms to filter out environmental interference and improve detection precision.
System Scalability	Utilize cloud-based infrastructure to handle growing data loads efficiently. Incorporate modular hardware components, allowing for incremental scaling as the number of users grows. Optimize database queries and implement load balancing to ensure consistent performance across multiple devices and users.
Flexibility in Integration	Design the system with open APIs to support seamless integration with various school management systems. Use standardized communication protocols to increase compatibility with future technologies. Include middleware or adapters to connect with legacy systems if needed.
Data Security	Implement end-to-end encryption for data both in transit and at rest. Incorporate multi-factor authentication and role-based access control to prevent unauthorized access. Regularly conduct security audits and introduce automated alerts for potential breaches.
Cost-Effectiveness	Opt for open-source software solutions and affordable hardware components without compromising quality. Use modular design to minimize upfront costs by allowing phased upgrades and expansions. Introduce predictive maintenance strategies to reduce long-term operational costs.
Ease of Use and Maintenance	Simplify the user interface by focusing on key functionalities and reducing unnecessary complexity. Provide automated system diagnostics and user-friendly maintenance tools. Develop comprehensive user manuals and quick-start guides to help users with minimal technical skills manage the system effectively.
System Functionality and Performance	Design with failover mechanisms to ensure continuity in case of device malfunctions. Incorporate offline mode features to maintain functionality in areas with poor connectivity. Continuously monitor system performance and provide real-time alerts for anomalies to prevent disruptions.

5.0 CONCLUSION

Existing IoT-based surveillance models for monitoring children present several weaknesses that limit their effectiveness and raise concerns. One of the primary issues is privacy, as these systems often collect sensitive personal data, including location information, which can be vulnerable to unauthorized access or data breaches if not properly secured. Additionally, the cost of implementing and maintaining such systems can be prohibitively high, particularly for schools with limited resources, as expenses include hardware, software, and regular maintenance.

Data security is another critical concern, as IoT devices are susceptible to hacking and cyberattacks, especially if encryption methods and security protocols are weak or outdated. Furthermore, these models heavily rely on stable network connectivity, and in areas with poor internet infrastructure, the system may experience disruptions, leading to delays or missed alerts. Inaccuracy and false alerts are also Common issues, as some systems may trigger unnecessary alarms when children are still within the designated safe zones, undermining trust in the system.

6.0 RECOMMENDATIONS

Schools should adopt IoT-based surveillance models to monitor students' real-time locations and attendance. This will improve student safety, especially in environments with high security concerns. Schools should start by implementing these systems in high-risk areas such as school gates, classrooms, and playgrounds.

Schools must ensure that student data collected through IoT surveillance systems is securely stored and handled. Schools should implement data privacy protocols to protect against data breaches, in compliance with government regulations. Staff should be trained on handling sensitive data responsibly.

7.0 REFERENCES

[1] The Constitution of Kenya, Aug. 27, 2010. [Online]. Available: https://www.refworld.org/docid/4c8508822.html. [Accessed: Jul. 13, 2021].

[2] J. J. Lomholt, J. N. Arendt, I. Bolvig, and M. Thastum, "Children with school absenteeism: Comparing risk factors individually and in domains," *Scand. J. Educ. Res.*, vol. 66, no. 3, pp. 411–426, 2021.

[3] A. Khaleel and S. Yussof, "An investigation on the viability of using IoT for student safety and attendance monitoring in Iraqi primary schools," 2016.

[4] A. Ahmed *et al.*, "An intelligent and secured tracking system for monitoring school bus," in *Proc. 2019 Int. Conf. Commun. Electron. Syst. (ICCES)*, 2019, pp. 1–5.

[5] M. Kassab, J. DeFranco, and P. Laplante, "A systematic literature review on Internet of things in education: Benefits and challenges," *J. Comput. Assist. Learn.*, vol. 36, pp. 115–127, 2020.

[6] Z. Jiang, "Analysis of student activities trajectory and design of attendance management based on internet of things," in *Proc. 2016 Int. Conf. Audio, Lang. Image Process. (ICALIP)*, 2016, pp. 600–603.

[7] H. F. Elyamany and A. H. AlKhairi, "IoT-school attendance system using RFID technology," *Int. J. Interact. Mobile Technol. (iJIM)*, vol. 14, no. 14, pp. 4–16, 2020.

[8] L. Lenz, A. Pomp, T. Meisen, and S. Jeschke, "How will the Internet of Things and Big Data analytics impact the education of learning-disabled students? A concept paper," in *Proc. 3rd MEC Int. Conf. Big Data Smart City (ICBDSC)*, 2016, pp. 1–7.

[9] Y. Wang, "The construction of the psychological health education platform based on Internet of Things," in *Appl. Mech. Mater.*, vol. 556, pp. 6711–6715, 2014.

[10] M. Georgescu and D. Popescu, "How could internet of things change the E-learning environment," in *Proc. 11th Int. Sci. Conf. eLearning Softw. Educ.*, 2015.

[11] P. Putjorn, C. S. Ang, and D. Farzin, "Learning IoT without the I-educational internet of things in a developing context," in *Workshop on Do-it-Yourself Networking: An Interdisciplinary Approach*, 2015, pp. 11–13.

[12] A. Jagtap, B. Bodkhe, B. Gaikwad, and S. Kalyana, "Homogenizing social networking with smart education by means of machine learning and Hadoop: A case study," in *Int. Conf. Internet Things Appl. (IOTA)*, 2016, pp. 85–90.

[13] A. El Mrabet and A. Ait Moussa, "IoT-based solutions for student attendance management: Applications and perspectives," *Int. J. Inf. Syst. Eng.*, vol. 8, no. 1, pp. 12–18, 2020.

[14] Z. Mouha, "Applications of IoT in improving the education and healthcare sectors," *J. Emerg. Technol.*, vol. 13, no. 2, pp. 45–58, 2021.

[15] S. Perwej, S. K. Perwej, and R. Perwej, "IoT middleware: A systematic review," in *Proc. Int. Conf. Recent Trends Electron. Commun. Eng. (RTECE)*, 2019, pp. 567–572.

[16] F. Ahmed, M. S. Ali, and T. I. Khan, "Dual authentication for school bus monitoring," in *Proc. IEEE Int. Conf. Mobile Comput. Security (ICMCS)*, 2019, pp. 1–7.

[17] S. Tamilselvan *et al.*, "Touch-free attendance system for COVID-19 safety using RFID and sensors," *J. Adv. Sci. Eng.*, vol. 27, pp. 11–15, 2021.

[18] K. Ajayalakshmi, V. Rajesh, and B. Srinivasan, "IoT-enabled school bus monitoring system with safety alerts," in *Proc. Int. Conf. IoT Appl.*, 2021, pp. 22–27.

[19] M. Maturkar, A. Deokar, and P. Kumar, "RFID and GSM-based bus tracking system for student safety," *IEEE Commun. Lett.*, vol. 24, no. 10, pp. 2342–2346, 2020.

[20] A. Tesfaye, "Real-time child tracking using GPS-enabled tags," *J. Emerg. Technol. Educ.*, vol. 9, no. 3, pp. 31–40, 2020.

[21] S. Senthamilarasi, R. Balasubramani, and M. Kumaravel, "Comprehensive IoT-based child safety monitoring system," *Int. J. Eng. Res.*, vol. 8, pp. 89–94, 2019.

[22] F. Dian, Z. Zhang, and Y. Ma, "Challenges of wearable IoT sensors in education and child safety," *Sensors Actuators*, vol. 12, no. 5, pp. 312–324, 2020.

[23] Q. Wu, J.-M. Redouté, and M. R. Yuce, "Energy-efficient designs for wearable IoT sensors," *IEEE Internet Things J.*, vol. 4, no. 3, pp. 791–799, 2017.

[24] W. Chen, L. Wang, and H. Li, "Design considerations for wearable IoT devices in education," *IEEE Access*, vol. 5, pp. 25668–25676, 2017.

[25] R. Lomotey, P. Sofranko, and R. Orji, "Security and privacy concerns in wearable IoT devices," *J. Syst. Softw.*, vol. 158, pp. 110–119, 2018.